**TREVOTECH PROJECT FOR CYBERSECURITY**

**TASK 1: Information Gathering**

With the use of NMAP and LEGION, Carry out reconnaissance on the following IP/Website targets:

1. https://www.aliexpress.com/

2. https://jumia.com/

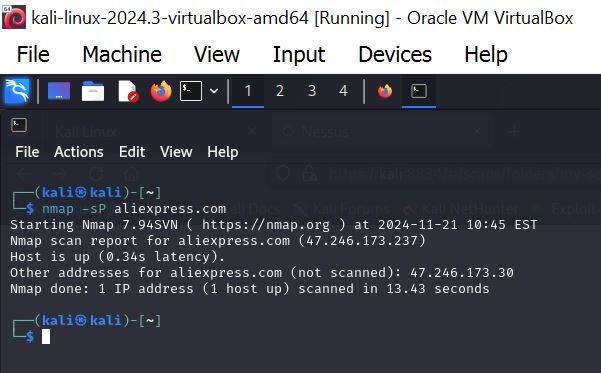
3. https://www.scrd.ca/

Draft in your responses as a report stating:

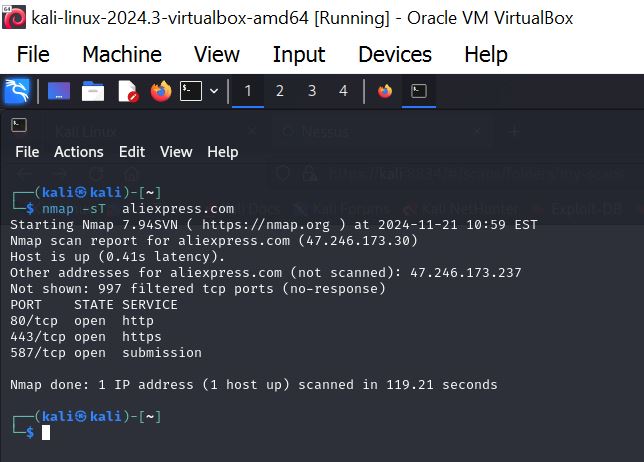
* Open Ports
* Services and the versions on the Opened ports
* Windows version
* Vulnerabilities associated with the Opened ports and the services.

**ANSWER USING NMAP**

Using Nmap to perform reconnaissance on the following IP/website, the result are as follows:

1. For <https://www.aliexpress.com/> we will start by identifying the response system using the ping scan, nmap -sP flag 

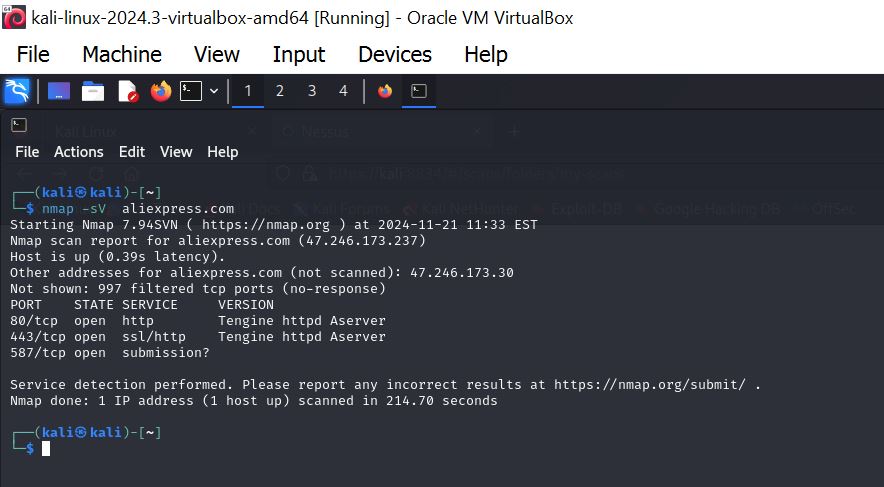
From the above we can see that the host IP is alive and running. Now we go ahead to check for **open port** using the TCP handshake scan(using the -sT flag).

 From the above image we were able to discover the open port, the state and their service.

There are three open ports on the network which are:

1. Open Port 80/TCP
2. Open Port 443/TCP
3. Open Port 587/TCP

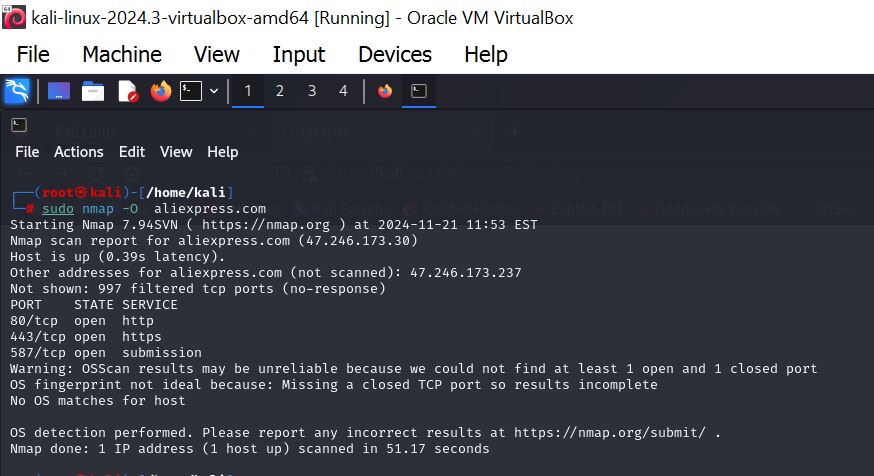
For the version and service of the open port, we will use the nmap -sV flag.



The image above shows shows us the server version and services for the open port. Both Port 80 and Port 443 are running on the same version “**Tengine httpd Aserver”.**

The service for Port 80 is http while that of Port 443 is ssl/http.

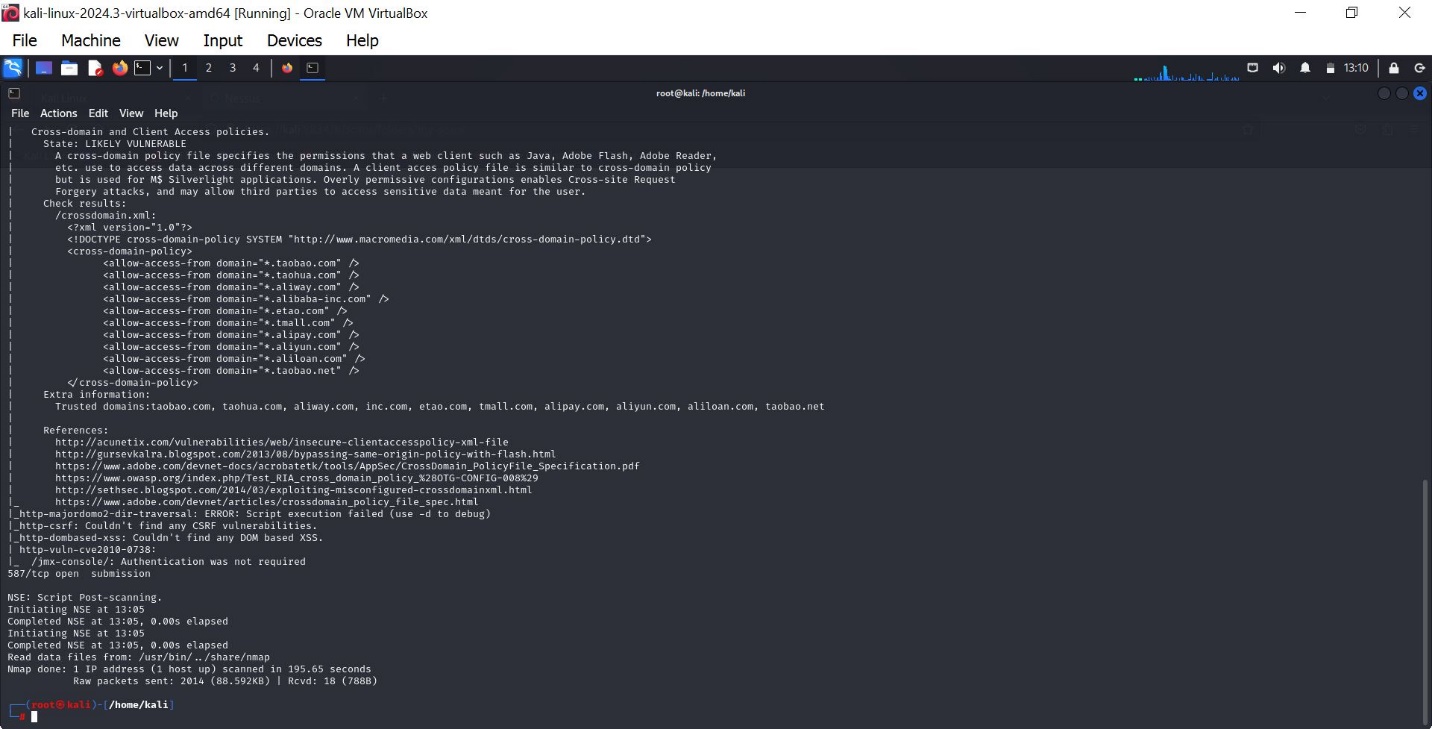
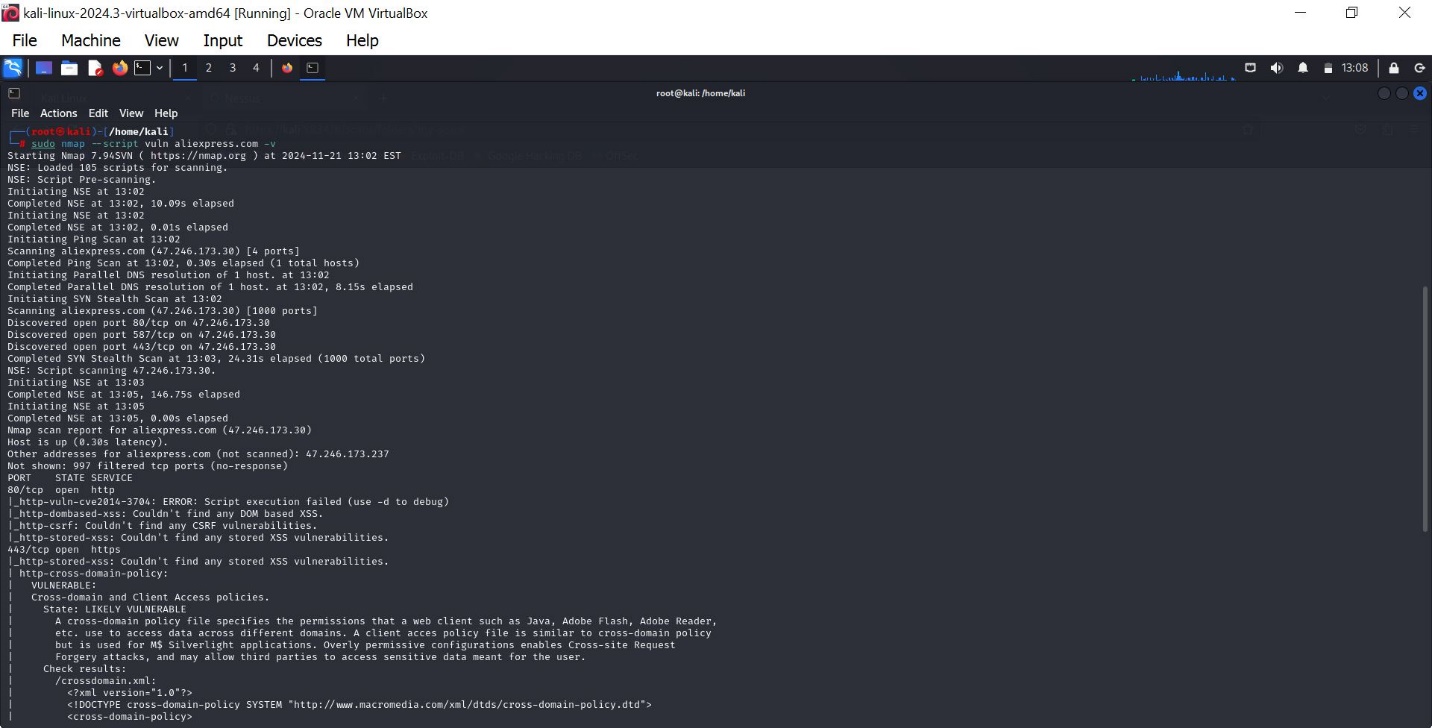
The window version can be checked using the nmap -O flag.



After performing the command to check the OS version on the network, the above image shows that nmap was unable to find the OS for the network IP.

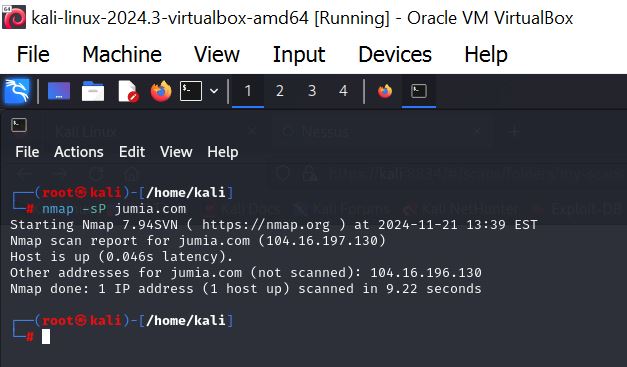
Next we will be checking for vulnerability associated with the open port and service.

To check for vulnerability we will using the command “sudo nmap –script vuln aliexpress.com -v”, the ‘-v’ indicate verbose. Below are images of the scan conducted.



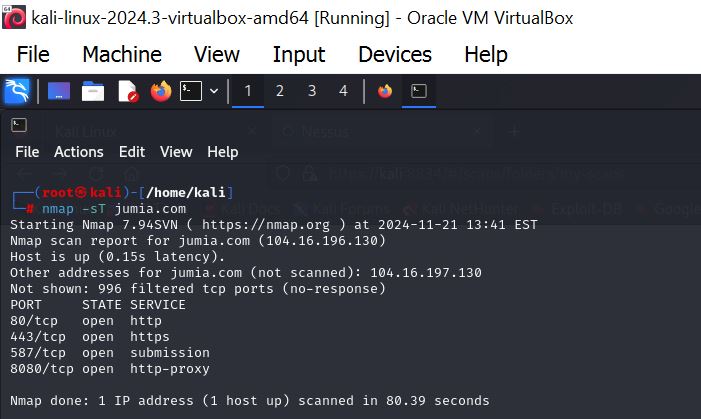
From the above images the result from the scan indicates that there is a vulnerability called **Cross-Domain and Client Access Policies** which tend to be likely vulnerable to the system

1. For <https://jumia.com/> we will start by using same procedure by checking if the target IP is up and running.



The images the host IP is up and running

Next we check for open port using nmap -sT flag command



We can see that the there is 4 open port on the network.

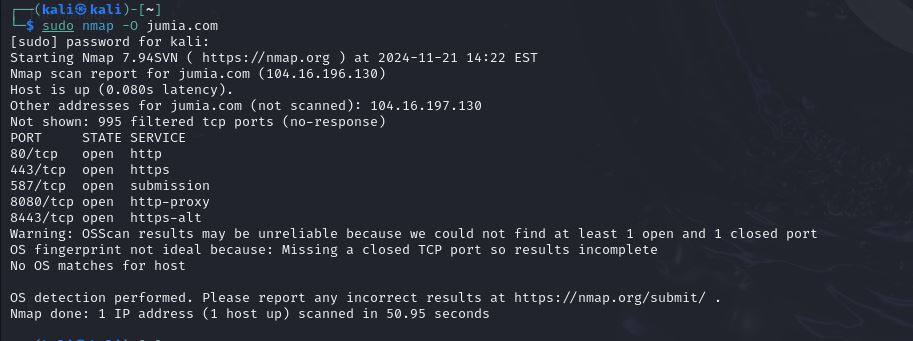
There are three open ports on the network which are:

1. Open Port 80/TCP
2. Open Port 443/TCP
3. Open Port 587/TCP
4. Open Port 8080/TCP

To check the services and version of the open port we use the nmap -sV flag command

From the image below we could not get the version of the website because it always appear to be down when trying to find the version.

Finding the windows version of the website



Nmap was unable to find the windows version with a result saying that ‘No OS matches for host’.

For the vulnerable check using verbose flag.

A screenshot of a computer

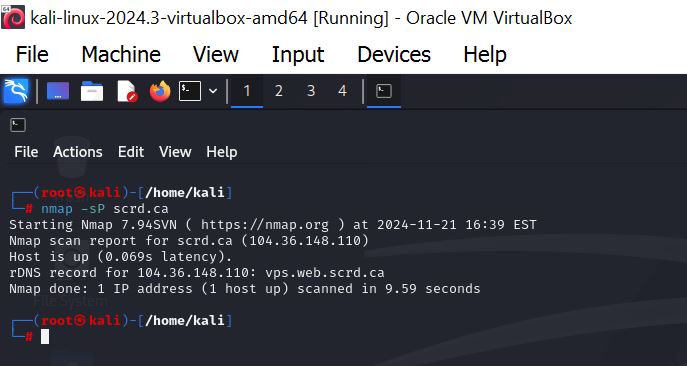
Description automatically generated

A screenshot of a computer

Description automatically generated

From the vulnerability scan of <https://www.jumia.com> the result shows that there is likely to be a vulnerability called Slowloris DOS Attack with CVE ID: CVE-2007-6750.

1. Performing reconnaissance on <https://www.scrd.ca/>. check if the host is up and running.

The host is alive and running.

We will be scanning for Open Port using the TCP handshake scan

A computer screen with white text

Description automatically generated

From the above image we can see that there are 11 open ports out of 15 ports on the network. The open ports are:

1. 26/tcp open rsftp

2. 53/tcp open domain

3. 80/tcp open http

4. 110/tcp open pop3

5. 143/tcp open imap

6. 443/tcp open https

7. 465/tcp open smtps

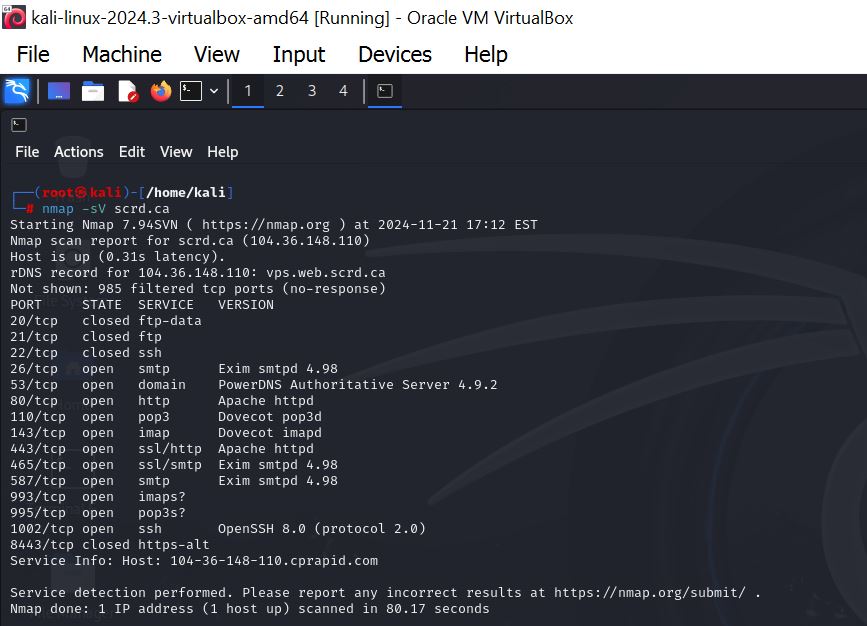
8. 587/tcp open submission

9. 993/tcp open imaps

10. 995/tcp open pop3s

11. 1002/tcp open windows-icfw

Service and Version of the open port on scrd.ca using the nmap -sV flag

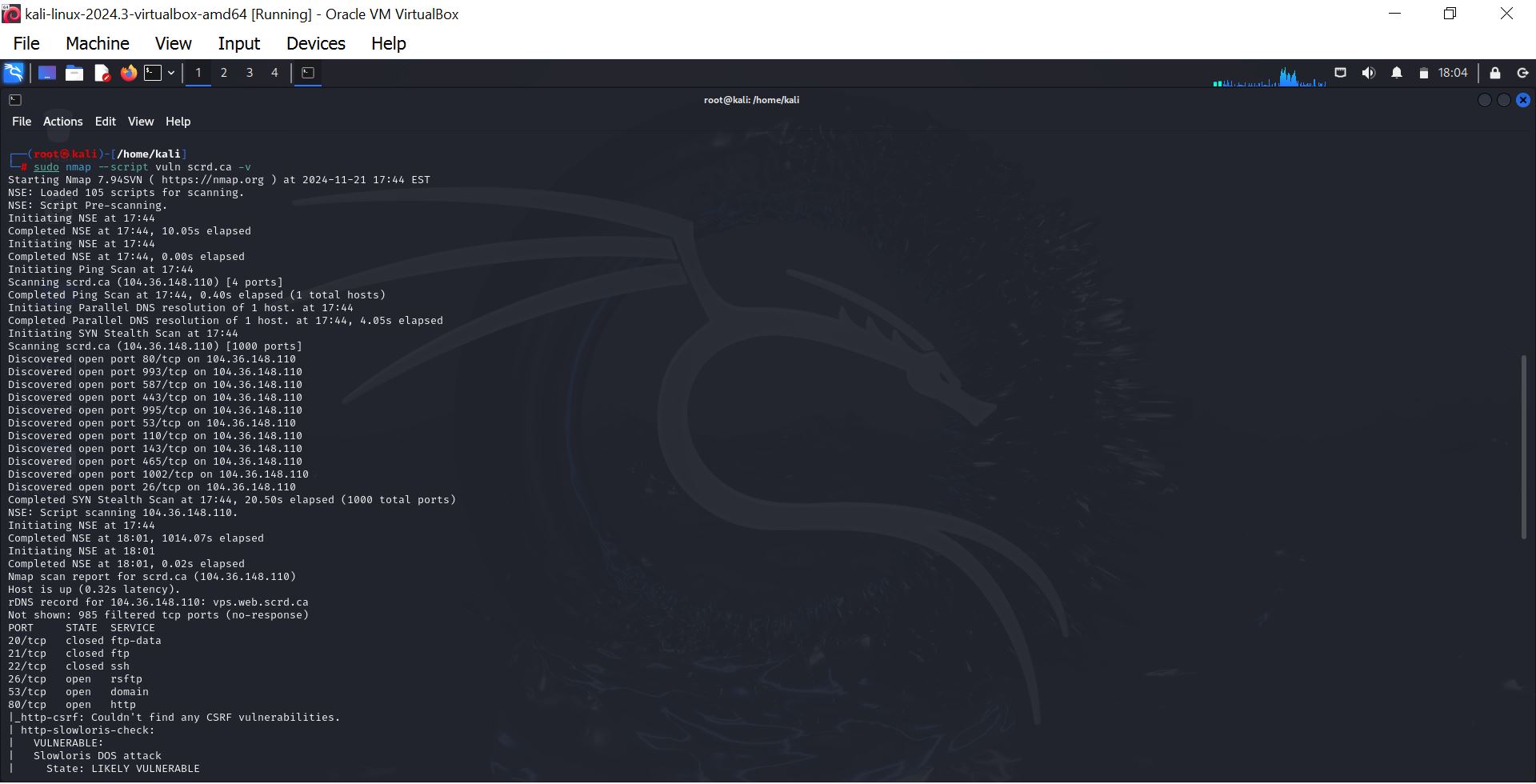
 The scan result shows of open port service and their server version.

Using the nmap command to scan for the OS version of the Host IP



From the above result the scan shows us that the OS is Linux with 92% guessing rate.

Lastly performing the vulnerability scan for the host website



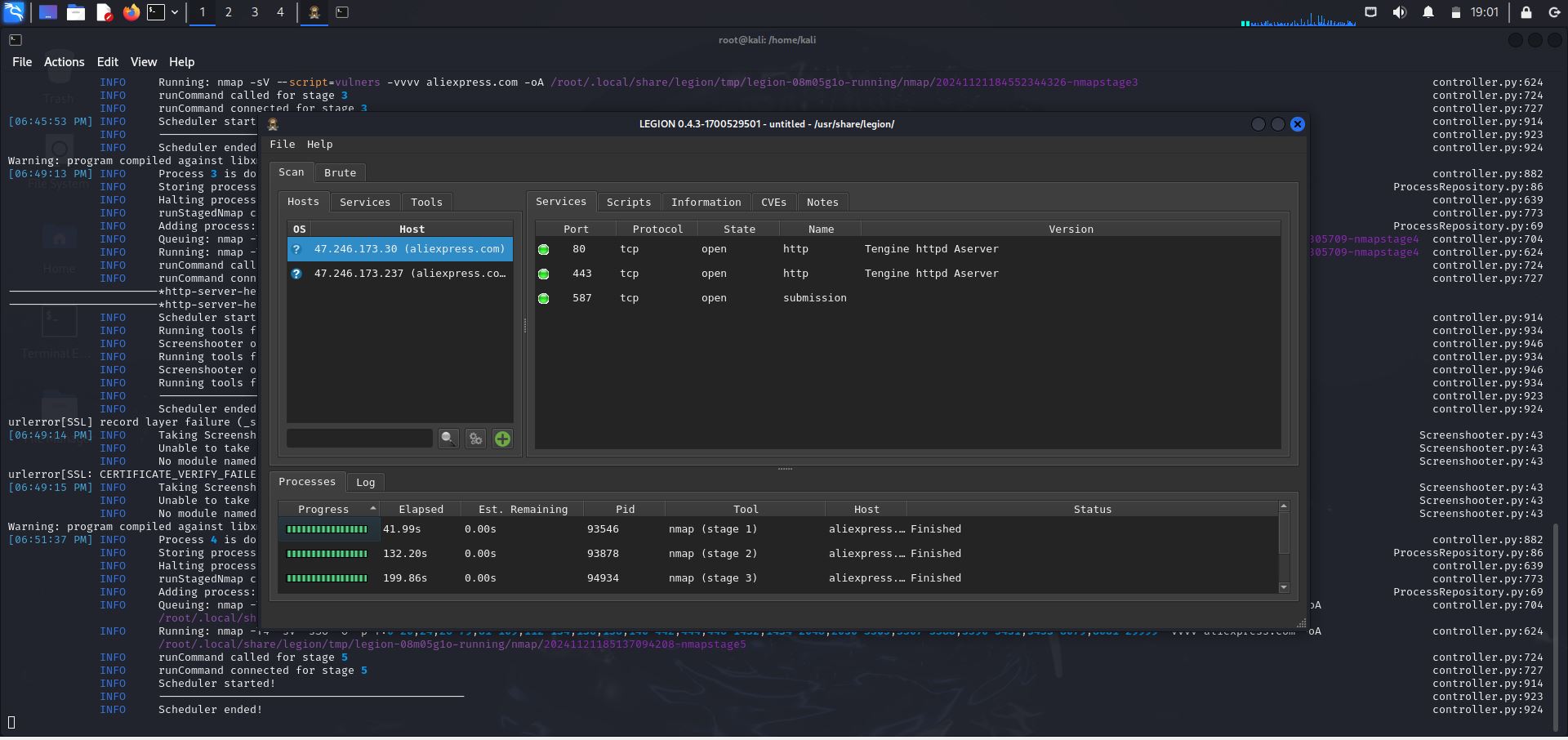
A screen shot of a computer

Description automatically generated

From the scan conducted, one(1) vulnerabilities(Slowloris DOS Attack with CVE ID: CVE-2007-6750) was spotted twice from the result.

**ANSWERS USING LEGION**

1. Performing reconnaissance on <https://www.aliexpress.com/> , the open ports, service and version of open port can be seen using the Legion software to scan. See image below

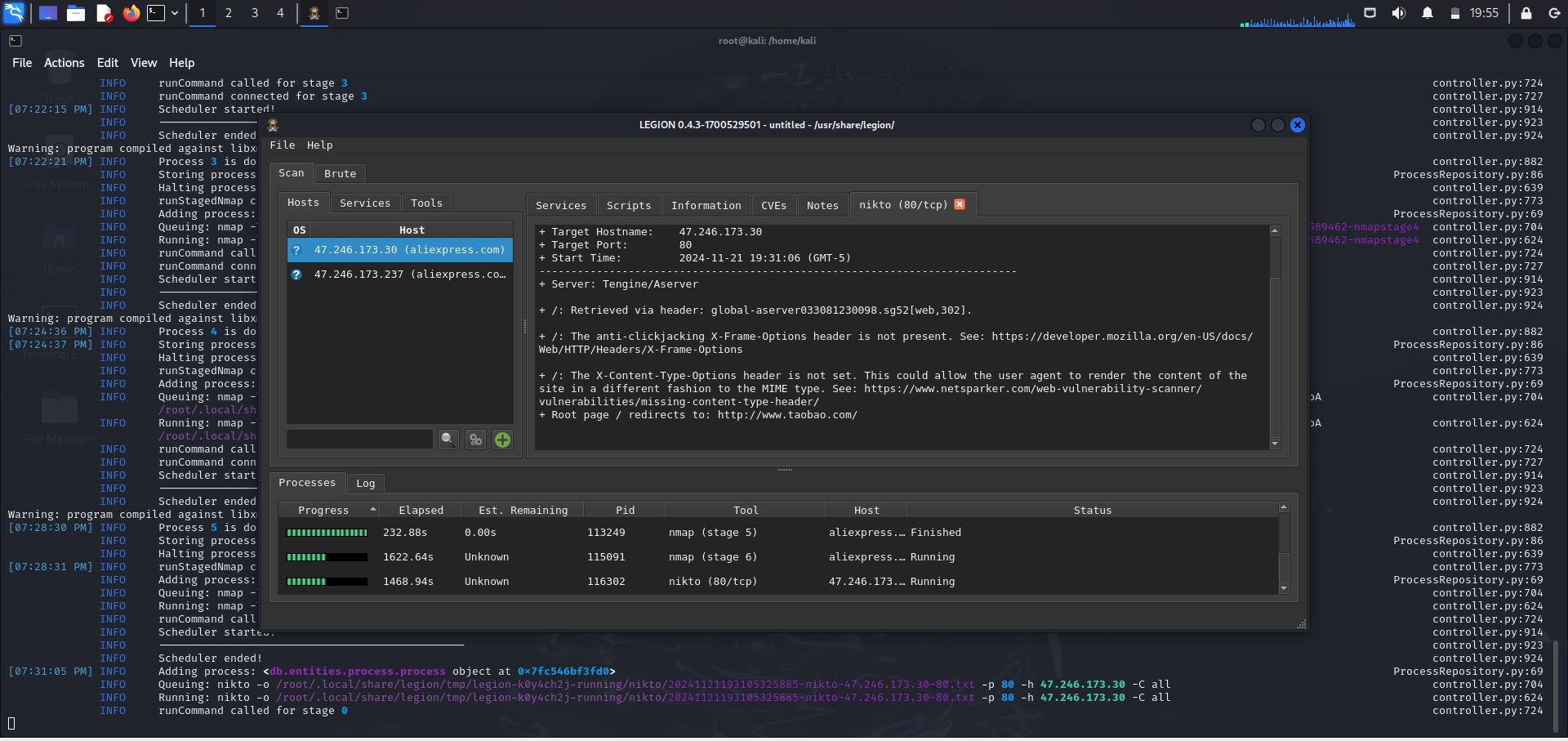


Below is an image of the OS of the host ip

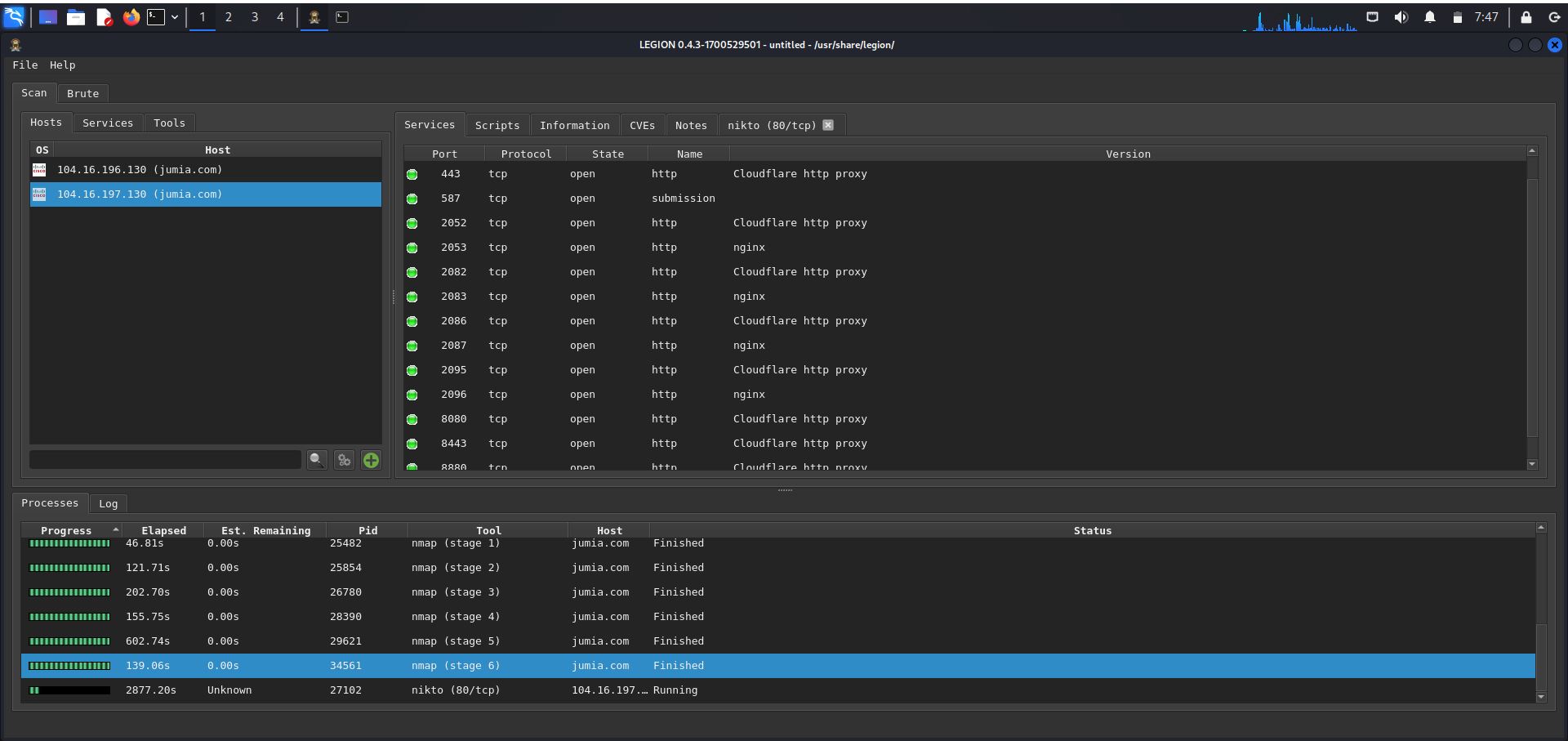
A screenshot of a computer

Description automatically generated

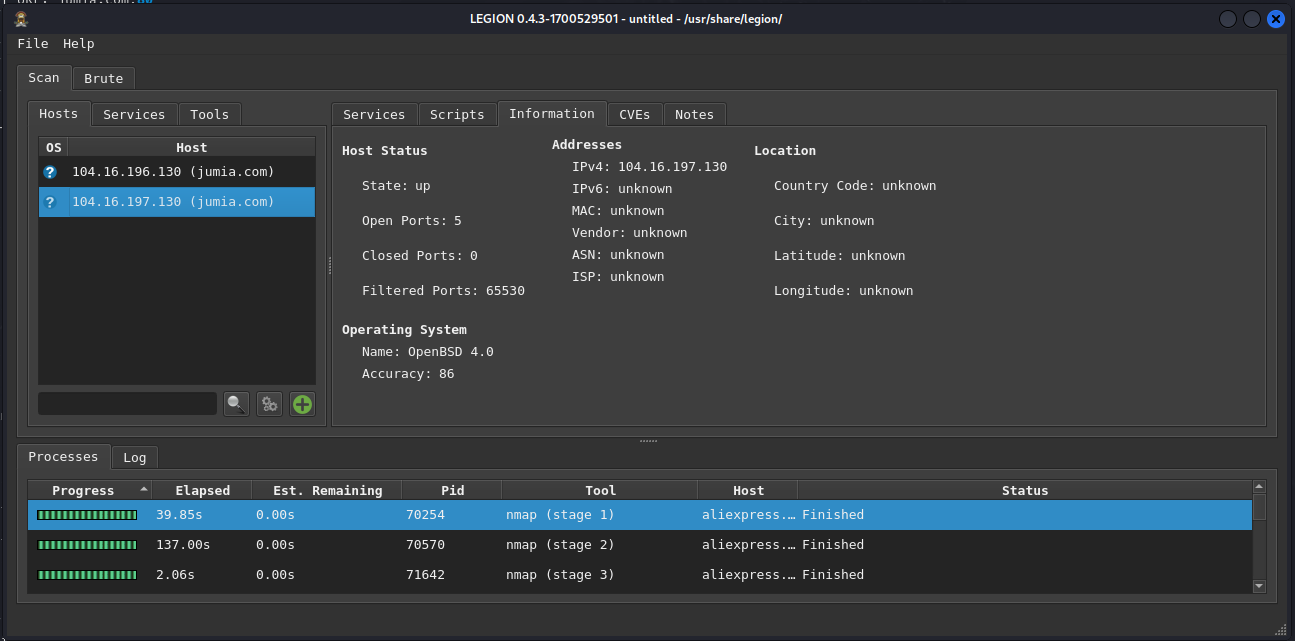
To get the vulnerability of the open port, Run the port with nikita, every vulnerability will be seen on the nikita’s tab.



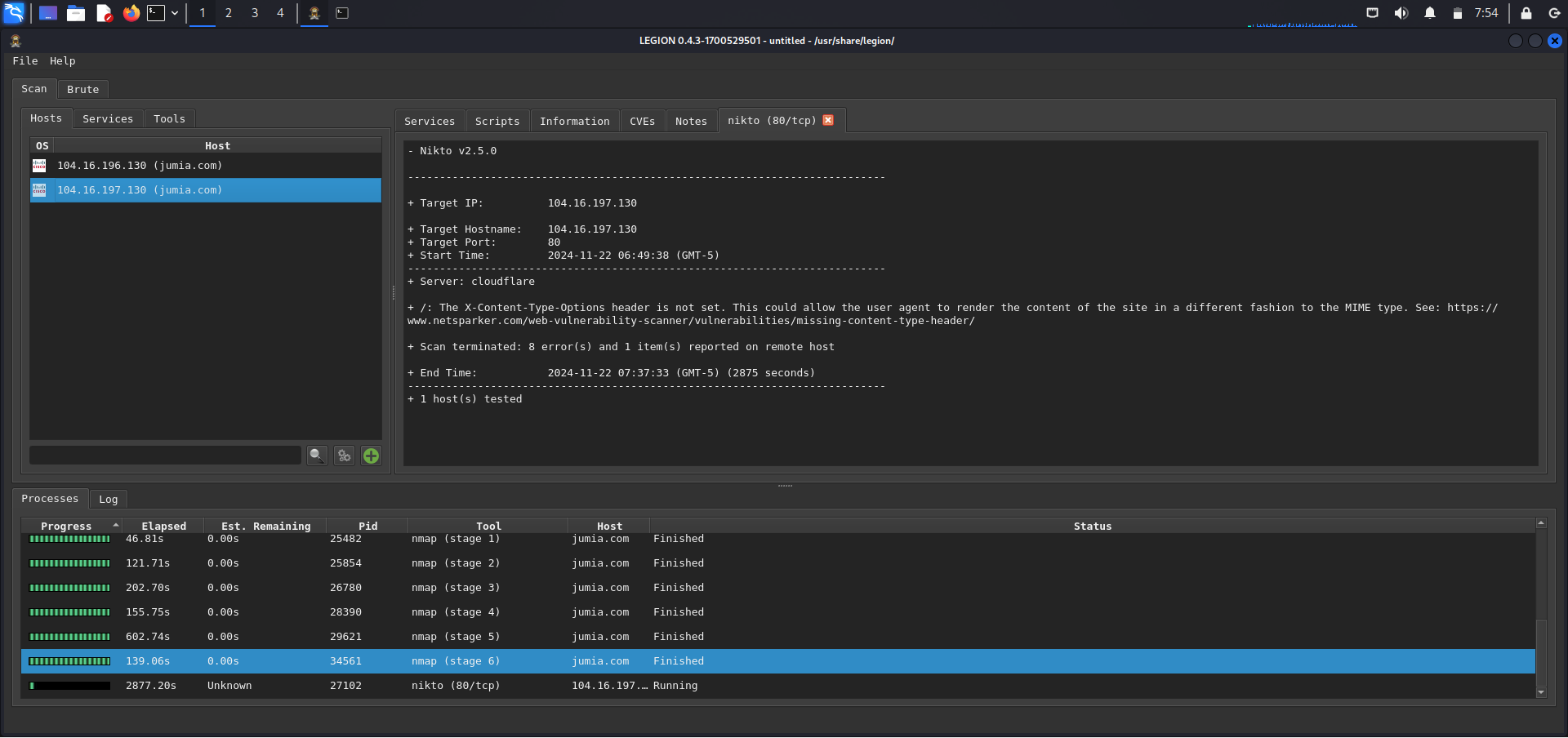
1. Performing reconnaissance on <https://www.jumia.com> using the legion software.



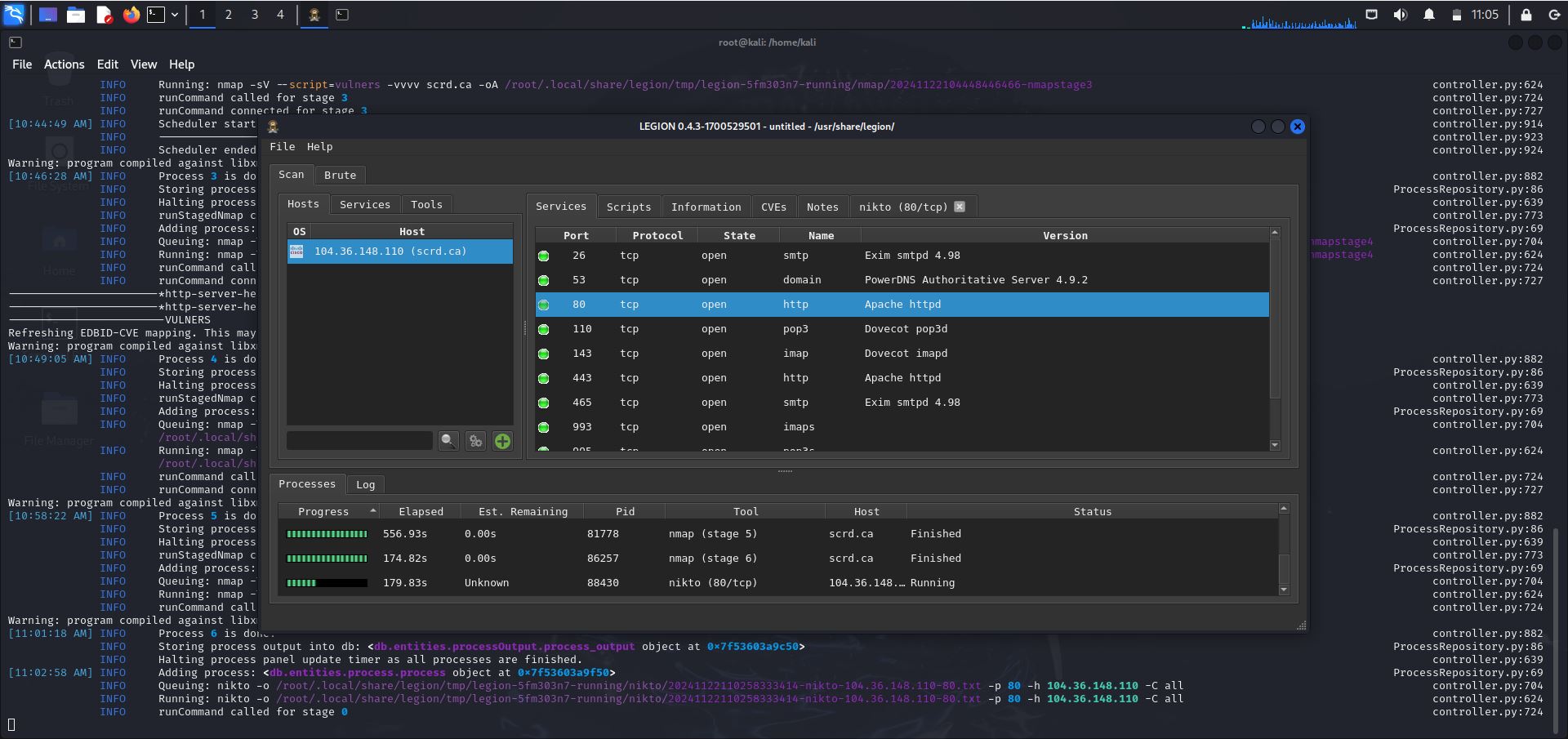
The image above shows a scan result with legion on jumia.com, we can see the open ports, their services and version.

Legion was able to detect the Operating system of the host with 86% accuracy

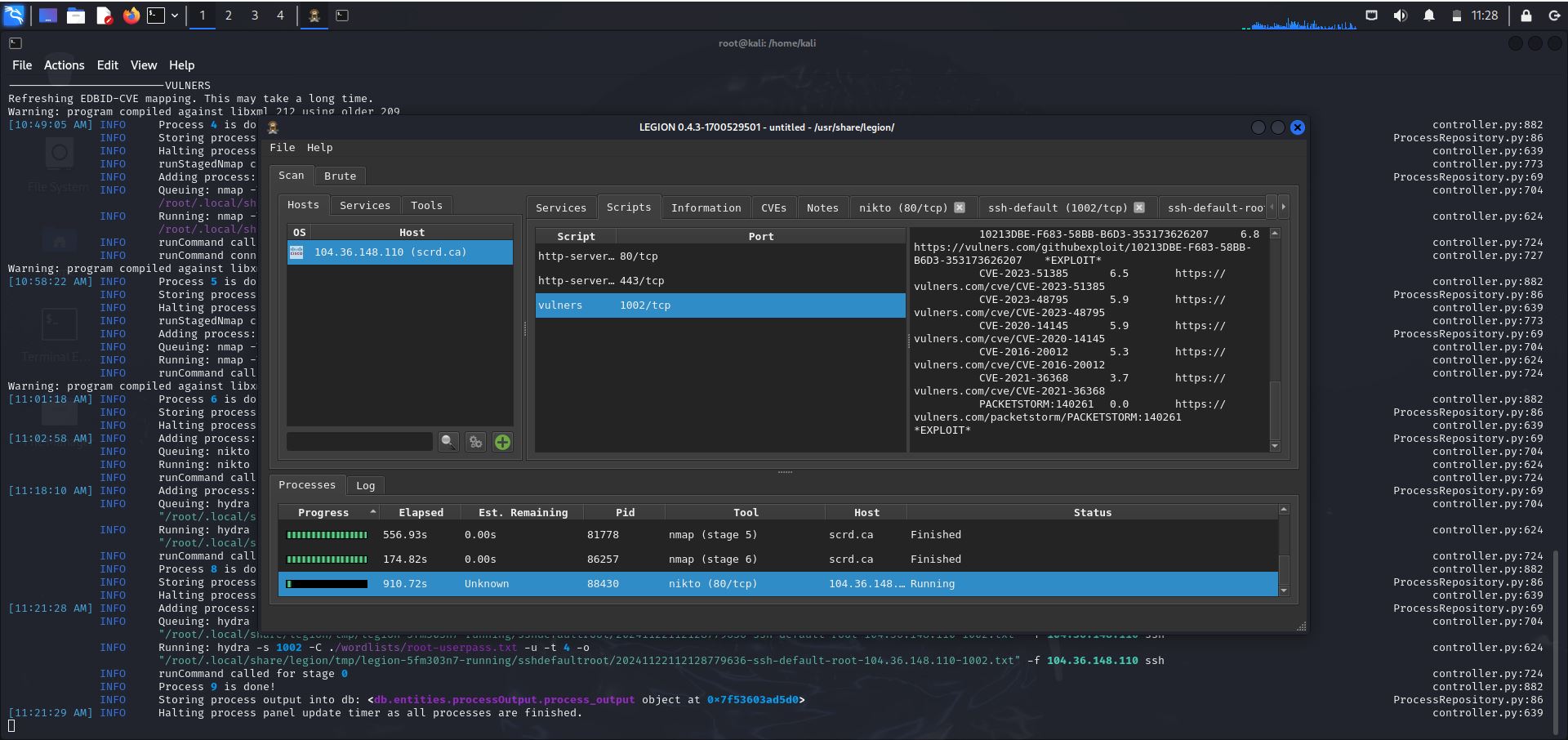
Now we go ahead and check for the vulnerability using nikita



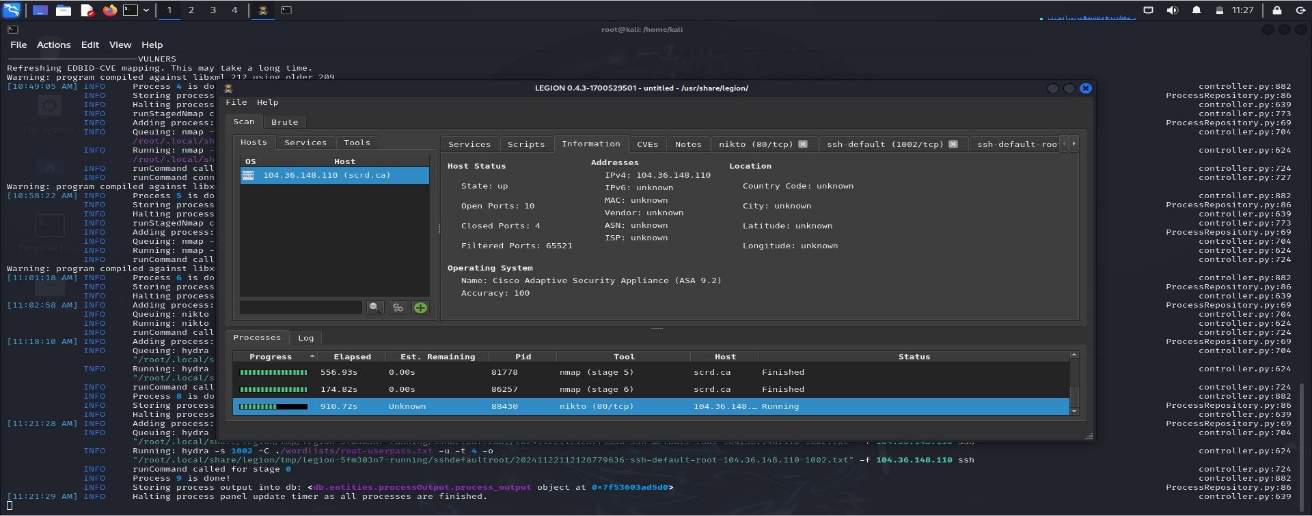
1. **Performing reconnaissance on** [**https://www.scrd.ca**](https://www.scrd.ca) **using legion. Below is an image showing the open ports, service and their version**



The script was checked and vulnerability data was picked from open port 1002/tcp below is an image on the scripts



Also the network information was able to give more insight about the network, which includes the open and closed ports, OS and IP. See image below



Below is an information about the default root credentialsA screenshot of a computer

Description automatically generated

Checking for vulnerabilities with nikita, below is an image showing the scan with nikita

A screenshot of a computer

Description automatically generated